(19)日本国特許庁（ＪＰ）　(12) 公表特許公報（Ａ）　(11)特許出願公表番号
特表2000－509451
（P2000－509451A）
(43)公表日　平成12年７月25日(2000.7.25)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ'(参考)
Ｅ０５Ｂ　49/00		Ｅ０５Ｂ　49/00	Ｈ

審査請求　未請求　予備審査請求　有　（全 20 頁）

(21)出願番号　特願平9－537774
(86)（22)出願日　平成９年４月15日(1997.4.15)
(85)翻訳文提出日　平成10年10月19日(1998.10.19)
(86)国際出願番号　ＰＣＴ／ＦＲ９７／００６７６
(87)国際公開番号　ＷＯ９７／４０４７３
(87)国際公開日　平成９年10月30日(1997.10.30)
(31)優先権主張番号　９６／０４９６３
(32)優先日　平成８年４月19日(1996.4.19)
(33)優先権主張国　フランス（ＦＲ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＡＵ，ＣＡ，ＪＰ，ＵＳ

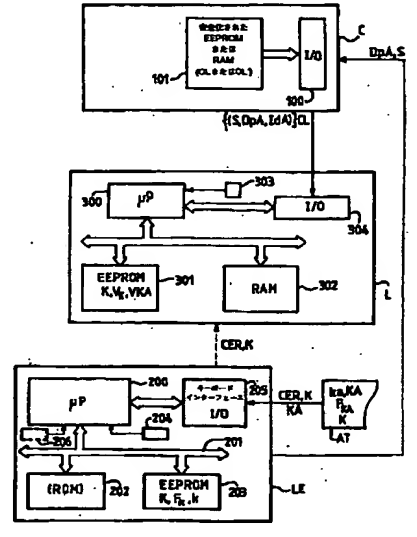
(71)出願人　ラ　ポスト
フランス国　92777　ブローニュービヤン　クール　セデックス　ケ　ドュ　ポワンー　ドュージュール　4
(72)発明者　ゲラン，ディディエ
フランス国　14000　カーン　リュ　コンスタン一フォルジュ　17
(72)発明者　アルディ，コンスタン
フランス国　92140　クラマール　リュ　デ　ヴォロンテール　9
(74)代理人　弁理士　越場　隆

最終頁に続く

(54)【発明の名称】　盗まれたり、なくした電子キーを自動的に無効にすることおよび／またはキーを生成する権限を転送することを可能にする安全化されたアクセス監視システム

(57)【要約】
本発明の対象はユーザの識別用のデータ要素を含む１つの電子キー（ＣＬ）（このキーは１つの生成手段（ＬＥ）によって生成される）が記録されている１つのポータブル記憶キャリヤ（Ｃ）と、上記記憶キャリヤがそれに必要な電子キーを含む場合にアクセスを許可することができる電子ロック（Ｌ）機能を満たす手段とによるアクセス監視の安全化されたシステムにある。本発明では、１つの論理キーＣＬは１つの特有のデータ要素Ｄ，Ａと、その署名Ｓとを含み、最初に使用する時に上記ロック（Ｌ）に記録される。ユーザがこのキーＣＬが記録された上記キャリヤ（Ｃ）を失うと、１つの新しいキーＣＬ'が別のキャリヤに記録され、この新しいキーを上記ロックに記録して上記の古いＣＬに重ね書きする。キーＣＬを生成する１つの権限を１つの生成手段ＬＥから別の生成手段へ転送するために、１つの新しい公開キーＫ'およびこのキーの署名ＣＥＲ'は別の生成手段にロードされる。ビルの管理での利用。

FIG_1



1

【特許請求の範囲】

１．ユーザの識別用のデータ要素を含む電子キーＣＬが記録されているポータブル記憶キャリヤ（Ｃ）と、上記記憶キャリヤが必要な電子キーを含む場合にアクセスを許可することができる電子ロック（Ｌ）機能を満たす手段とによるアクセス監視のシステムにおいて、　－上記電子キーＣＬが、上記ユーザおよび上記キャリヤに特有のデータ要素D_pAと、これらのデータ要素のデジタル署名Ｓとを含み、　－これらのデータ要素が上記キャリヤを最初に使用する時に上記ロックに記録され、　－上記キャリヤが失われたあるいは盗まれた場合には、新しい電子キーＣＬ’が生成され、このキーが同一のユーザ用の新しい記憶キャリヤに記録されて、新しい特有のデータ要素D_pA'は古いデータ要素より高い値を有し、上記の古いデータ要素を無効にし、　－上記キャリヤを使用するたびに、上記ロック（Ｌ）が上記デジタル署名Ｓを検証し、上記キャリヤの上記キーＣＬの特有のデータ要素D_pAが既に記録された上記データ要素に等しいかまたはそれ以上であることを確認してこれらの条件が合う場合にのみアクセスを許可することを主に特徴とするシステム。２．上記署名Ｓが、秘密キーｋを有するアルゴリズムと、対応する公開キーＫとから生成手段ＬＥによって計算されること、および上記ロックが、メモリ内に、上記公開キーＫと、この署名Ｓの検証用の関数（V_K）と、この検証関数を実施する手段とを有することを特徴とする請求項１に記載のアクセス監視システム。３．ユーザに特有のデータ要素D_pAを検証するために、上記ロックは：－上記キャリヤに存在する上記の特有のデータ要素D_pAと、このユーザの最初の使用時に既に記録された上記データ要素とを比較し、－このデータ要素の値が既に記録された上記データ要素より大きい場合は、このデータ要素を既に記録された上記データ要素に代えて記録することを特徴とする請求項１または２に記載のアクセス監視システム。４．ユーザＡのキャリヤに割り当てられた上記の特有のデータ要素（D_pA）が、ユーザＡの記憶キャリヤのカスタム化の日付であることを特徴とする請求項１～３のいずれか一項に記載のアクセス監視システム。５．上記の特有のデータ要素D_pAが、カウンタ（206）によって得られる値であり、この値が所定のユーザのキーの新しいバージョンごとに増加することを特徴とする請求項１～４のいずれか一項に記載のアクセス監視システム。６．上記電子ロック（Ｌ）が基準値（ＤＨ）を有し、アクセスの許可が、キャリヤに特有の上記データ要素D_pAが上記基準値より小さい値の場合にのみ与えられることを特徴とする請求項１～５のいずれか一項に記載のアクセス監視システム。７．上記基準データ要素ＤＨが、上記電子ロックの１つの内部クロック（303）によって与えられる上記の現在の日付であることを特徴とする請求項１～６のいずれか一項に記載のアクセス監視システム。８．上記生成手段

2

が、上記キーＣＬを生成する認証機関によって与えられる権限情報要素ＨＡを有し、この権限情報要素ＨＡが識別要素ＩＤと、公開キーＫと、有効期間ＶＡＬと、このキーのデジタル署名ＣＥＲとを含むこと、および権限の転送が、新しい公開キーＫ’およびそれに対応する署名ＣＥＲ’を記録することによって新しい生成手段に対して行われることを特徴とする請求項２に記載のアクセス監視システム。９．上記古いキーＫに割り当てられた有効期間の終了日が、上記新しいキーＫ’の有効期間の有効性の開始の日付に対応するか、またはこの開始の日付以降の日付であることを特徴とする請求項８に記載のアクセス監視システム。１０．署名ＣＥＲ’を有する新しいバージョンのキーＫ’を検証するために、上記ロックは公開キーを有する検証機能を使用し、上記ロックは古いキーの有効期間の終了の日付と、次のキーの有効性の開始の日付とを比較してこれらを置換することを特徴とする請求項８および９に記載のアクセス監視システム。１１．電子キーＣＬの検証中に、上記ロックは：－上記のカスタム化の日付D_pAと、使用されている公開権限キーＫの有効性期間ＶＡＬとを比較する操作と、－この日付がこのキーの有効期間内にある場合は、アクセスを許可し、それ以外の場合はアクセスを拒否する操作とを行うことを特徴とする請求項１～１０のいずれか一項に記載のアクセス監視システム。１２．上記の公開キーが、公開キーＫＡを有する１つの生成関数F_KAによって認証機関で得られ、上記ロックがメモリ内に、権限の検証時に、検証関数V_{KA}および上記キーＫＡを含む請求項１～１１のいずれか一項に記載のアクセス監視システム。

【発明の詳細な説明】

盗まれたり、なくした電子キーを自動的に無効にすることおよび　／またはキーを生成する権限を転送することを可能にする安全化　されたアクセス監視システム

本発明は、盗まれたり、なくした論理キーを自動的に無効にすることおよび／またはキーを生成する権限を転送することを可能にするアクセス監視の安全化されたシステムに関するものである。　本発明は特に、ビル、コンピュータシステムあるいは開放または使用を監視しなければならない任意の物へのアクセスを監視する分野に適用することができる。　許可され、更新可能なタイムスロットに制限されるアクセス監視システムとしては、国際公開番号WO96/029899として公開された特許出願PCT/FR95/00935が知られている。　このシステムは、フラッシュコンタクト有りまたは非接触のチップカード（集積回路カード）、磁気カード、バッジおよび電子キー（接触してもしなくてもよい）などのポータブル記憶キャリヤの使用に依存する。これらのキャリヤはアクセスを許可された全てのユーザに配布される。　このために、上記磁気キャリヤはアクセスの権限を与える記憶された電子キーを有する。　このキーは、１つのアクセス許可時

間に対応する１つのデータ要素およびこのデータ要素の１つのデジタル署名を有する。使用時間は、実際には使用する日および使用するタイムスロットに対応し、したがって上記キーはある日の特定のタイムスロットの間でのみ有効である。　これらのキーの寿命は短いので、ポストマンによるメールの配達および収集などの用途に特に適している。このようなキャリヤのユーザは、新しい有効キーを自分のキャリヤに毎日ロードしなければならない。　この論理キーの寿命は一過性であるので、このようなキーを含む情報キャリヤの盗難または損失の問題はなくなる。　このキャリヤを見つけたあるいは盗んだ人はその翌日にはこれを使用することはできなくなる。その結果、盗まれたあるいは失われた全てのキャリヤのブラックリストを維持する必要さえなくなる。　このアクセス監視システムは恒久的なアクセス権または極めて長期的なアクセス権を提供する必要がない用途において非常に有効である。しかし、それ以外の場合にはこのシステムは適していないことがわかる。　以前の監視システムでは、盗まれたり、なくしたキャリヤのブラックリストを維持して、このようなキャリヤを持つすることを許可されていないのにこのようなキャリヤ持っている者が保護されたユニットにアクセスするのを防ぐ方法を提案している。　このようなリストの維持は電子ロックへの作用を必要とする。なぜなら盗まれたり、なくしたキャリヤの識別番号をこのキャリヤの保持者がその亡失を報告した後にこれらのロックに記録する必要があるからである。このような作用は制約を伴う。　本発明の目的はこの問題を解決することにある。　本発明の安全化されたアクセス監視システムではなくしたり、盗まれたと報告されたキーを自動的に無効にすることができる。　実際に、本発明では、電子ロックに対する特別な作用はない。この失われたあるいは盗まれたキャリヤを自動的に無効にすることができるのは、ユーザのキャリヤである。　さらに、電子キーを生成してこれらを上記記憶キャリヤに記録する権限を与えられた人が彼の権限を手放す場合（ビルへのアクセスの権限の場合では、例えばこのビルの管理代行業者または管理者の交替によって起こりうる）、別の人へ権限を転送することによって、新しい権限を有するキー生成手段を用いてこの電子キーを計算する新しいキャリヤを、アクセス権を所有していた全てのユーザに提供する必要がでてくる。　これはかなりのコスト高をまねく制約である。　本発明の安全化されたアクセス監視システムを用いることでこの問題を解決することもできる。送出されたキャリヤは、この権限が、別の人物、具体的には別のキー生成手段へ転送される場合でも、常に有効性を維持している。　本発明の目的は特に、ユーザの識別用のデータ要素を含む電子キー（ＣＬ）が記録されているポータブル記憶キャリヤ（Ｃ）と、上記記憶キャリヤが必要な電子キーを含む場合にアクセスを許可することができる電子ロック（Ｌ）機能を満たす手段とによるアクセス監視のシステムにおいて、　－上記電子キーが、上記ユーザおよび上記キャリヤに特有のデータ要素D_pAと、これらのデータ要素のデジタル署名Ｓとを有し、　－これらのデータ要素が上記キャリヤの最初に使用する時に上記ロックに記録され、　－上記キャリヤが失われたり、盗まれた場合には、新しい１つの電子キーが生成され、このキーがこの同じユーザ用の別の１つの記憶キャリヤに記録されて、新しい特有のデータ要素は古いデータ要素より高い値を有し、上記の古いデータ要素を無効にし、　－上記キャリヤを使用するたびに、上記ロック（Ｌ）が上記デジタル署名Ｓを検証し、上記キャリヤの上記キーＣＬの特有のデータ要素D_pAが既に記録された上記データ要素に等しいかそれ以上であることを確かめてこれらの条件が合う場合にのみアクセスを許可することを主に特徴とするシステムにある。　別の特徴では、上記署名Ｓは１つの秘密キーｋを有するアルゴリズムと、対応する１つの公開キーＫとから生成手段ＬＥによって計算され、上記ロックは、メモリ内に、上記公開キーＫと、この署名Ｓの検証のための関数V_Kと、この検証関数を実施する手段とを有する。　別の特徴では、ユーザに特有のデータ要素D_pAを検証するために、上記ロックは：－上記キャリヤに存在する上記の特有のデータ要素D_pAと、このユーザの最初に使用する時に既に記録されたデータ要素とを比較し、－このデータ要素の値が既に記録された上記データ要素より大きい場合は、このデータ要素を既に記録された上記データ要素の代わりに記録する。　ユーザに特有の上記データ要素D_pAは、彼の記憶キャリヤのカスタム化の日付にすることができる。　上記データ要素D_pAはカウンタによって得られる値にすることができ、この値は所定のユーザについてキーの新しいバージョンごとにインクリメントする。　これらの操作は、新しいキャリヤに特有の新しいデータ要素のを古いものの代わりに上記ロックに記録することによって、ユーザへ新しいキャリヤを発行したことを自動的に更新することができる。　１つの新しいキャリヤが所定のユーザ用にカスタム化される場合、上記の特有のデータ要素D_pA（上記カスタム化の日付）は古いものより大きい値を有する。　１つのキャリヤに記録された上記電子キーＣＬはこのキャリヤを識別するデータ要素を有する。例えば上記キャリヤの製造の通し番号である。　安全性を高めるために、上記電子ロックは基準値ＤＨに対応するデータ要素を有する。アクセスの許可は、さらに上記ユーザに特有の上記データ要素D_pAが上記基準値ＤＨより小さい値の場合にのみ与えられる。　上記の基準データ要素ＤＨは上記電子ロックの１つの内部クロックによって与えられる現在の日付である。　本発明の別の特徴では、上記生成手段は上記キーＣＬを生成する認証機関によって与えられる権限情報要素ＨＡを有し、この権限情報要素ＨＡは１つの公開キーＫと、この情報要素の

デジタル署名ＣＥＲとを含み；新しい生成手段への権限の転送が、新しい公開キーK’およびそれに対応する署名ＣＥＲ’を記録することによって行われる。　上記ロックは全ての新しい権限を検証する。　このために、全ての新しい公開キーは上記電子ロックに記録され、原則として維持されないその証明を用いて検証される。　別の特徴では、上記生成手段に属する上記データ要素は１つの識別データ要素ＩＤと、１つの有効性の時間ＶＡＬと、上記公開キーKとを含み、上記の古いキーKに割り当てられた上記の有効性の時間は、上記の新しいキーK’の有効性の時間の有効性の開始の日付に対応する終了の日付を有し、この終了の日付はこの開始の日付より後（例えば一月後）にすることもできる。　別の特徴では、１つの署名ＣＥＲ’を有する新しいバージョンのキーK’を検証するために、上記ロックは古いキーの有効性の時間の終了の日付と、次のキーの有効性の開始の日付とを比較してこれらを置換える。　１つの電子キーの検証中に、上記ロックはさらに下記の操作：－上記のカスタム化の日付D_pＡと、使用している公開権限キーKの有効性の時間ＶＡＬとを比較する操作－この日付がこのキーの有効性の時間内にある場合は、アクセスを許可し、それ以外の場合はアクセスを拒否する操作を行うのが有利である。　上記の公開キーK、K’は、１つの秘密キーｋａを用いて、公開キーＫＡを有する１つの生成関数F_{KA}によって認証機関によって得られる。上記ロックはメモリ内に、検証時に、上記署名ＣＥＲまたはＣＥＲ’を検証するための検証関数V_{KA}および上記キーＫＡを有する。　本発明の対象はさらに、電気キーＣＬが記録されている１つのポータブル記憶キャリヤＣと、これらの電子キーを生成するための手段と、上記記憶キャリヤがそれに必要な電子キーを有する場合にアクセスを許可することができる電子キー機能Ｌを実施する手段とによるアクセス監視用のシステムにあり、このシステムでは上記の生成手段が、上記キーＣＬを生成する権限用情報要素ＨＡを有し、この権限用情報要素ＨＡは１つの公開キーKと、この情報要素の上記デジタル署名ＣＥＲとを含み、さらにこのシステムでは新しい生成手段への権限の転送が、１つの新しい公開キーK’およびそれに対応する署名ＣＥＲ’を記録することによって行われる。この新しい公開キーは、上記の権限の検証後、上記電子ロックＬに記録され、この電子ロックＣＬは上記手段ＬＥによって生成された上記キーＣＬを検証する。　別の特徴では、上記生成手段に属する上記データ要素は１つの識別データ要素ＩＤと、１つの有効性の時間ＶＡＬと、上記公開キーKとを含む。１つの新しいキーK’に割り当てられた有効性の時間は、上記の古いキーKの有効性の時間の有効性の終了の日付に対応する開始の日付を有する。　１つの署名ＣＥＲ’を有する新しいバージョンの上記公開キーを検証するために、上記ロックはこの新しいキーの有効性の時間の開始の日付と、上記の古いキーの有効性の終了の日付とを比較するのが有利である。　上記の公開キーは、秘密キーｋａを用いて、公開キーＫＡを有する１つの生成関数F_{KA}によって認証機関によって得られ、上記ロックはメモリ内に、検証時に、これらの署名ＣＥＲまたはＣＥＲ’を検証するための検証関数V_{KA}および上記キーＫＡを有する。　したがって、１つの新しい生成手段の使用時には、この手段はこの手段によって生成されるキーを制御する上記ロックに宣言されている。　このために、上記認証機関は上記ロックおよびこの認証機関が計算に使用する上記キーＫＡに上記の権限証明を記録する。上記生成手段はそれ自体上記ロックにその権限を記録することができる。　許可されなくなった手段によって不正に生成されたキーを有する上記キャリヤは上記の保護されたユニットにアクセスすることはできない。　実際に、権限の転送は１つの新しい公開キーを上記ロックに安全にロードすることによって行われる。　上記の古い公開キーは上記生成アルゴリズムが破壊されたり、上記秘密キーと上記公開キーとによって生成された１対の秘密キーが発見されたりしない限り原則として保存される。　本発明の他の特徴および利点は添付図面を参照した以下の説明からより良く理解できよう。本発明は下記実施例に限定されるものではない。　図１は本発明の第１の目的の安全化されたアクセス監視システムを示し、　図２は本発明の第２の目的の安全化されたアクセス監視システムを示す。　「認証機関(authority)」という用語は秘密キーと、公開キーを送り出すことができる手段と、権限データ要素とを有する組織(organization)を意味するものとする。　「秘密キー」という用語はこの認証機関のユニットまたは生成手段にのみ知られているデジタルデータ要素を意味するものと理解される。　「公開キー」、ＫＡ，Ｋ，Ｋ’という用語は複数のユーザ、すなわち認証機関および電子キーの生成の手段または電子ロックの生成の手段によって共有されているデジタルデータ要素を意味するものと理解される。　キーの「生成手段」ＬＥという用語は、デジタルデータ処理機器、例えばマイクロコンピュータなどを意味するものと理解され、この機器は権限情報ＨＡを含み、従来の公開キーを有するアルゴリズム等の機能を実施するこのデジタルデータ信号を得るための計算手段を有する。　「電子キー」または「論理キー」ＣＬという用語は、アクセス権を与えるデジタル署名を伴う１つまたは複数のデジタルデータ要素を意味するものと理解される。　一例として、ビルへのアクセスの管理に本発明を適用して説明する。　より良く理解できるように図１を参照する。　許可されたユーザに配布されたこの電子キーを有するこの記憶キャリヤＣはチップカードまたはチップキーまたはバッジまたは磁気カードにすることができる。このキャリヤＣとロックＬとの間のこの伝送は電子的接触を通してまたは無線電気手段によってまたは磁気テープの読取りによって行うことができ

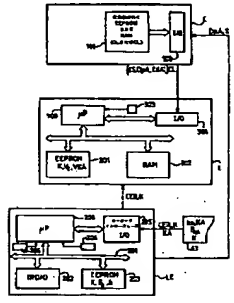
る。　一例を挙げると、キャリヤとしてはチップカードが選択される。　このチップカードは入力／出力インターフェースＩ／Ｏ100と、電気的に記録可能な不揮発性メモリ101を有する。　図示した実施例では、キャリヤＣのカスタム化は特に、メモリにユーザＡを識別するための情報要素ＩＤＡを記録することで構成されており、この情報要素は例えばユーザＡの名前、ユーザＡの部屋番号およびユーザＡに割り当てられた特有のデータ要素D_pAなどを含む。好ましい実施例では、このデータ要素ＤＡはユーザＡの記憶キャリヤのカスタム化の日付である。　このキャリヤを識別する情報要素のメモリでも記録は行われる。これは例えば、このキャリヤの製造シリアル番号ＮＳである。一般に、この情報要素は製造工程の最後、このキャリヤがこの認証機関ＡＴに引き渡される前に入力される。　このキャリヤのこのカスタム化は権限ＨＡ（ＩＤ，ＫＡ，ＣＥＲ，Ｋ）を有する機器ＬＥ（およびこの使用者）によって行われる。　この生成器ＬＥは、例えばカード読取り機を備えたＰＣ型のマイクロコンピュータによって形成される。　図１は、この機器ＬＥの各機能ブロックを概念的に示している。　この生成器ＬＥはバス２０１によってメモリに接続されたユニット２００を有するマイクロプロセッサ型である。ＲＡＭ型の揮発性作業メモリ202はアプリケーションのデータ要素を含む。　ＥＥＰＲＯＭ型の不揮発性メモリは、保護された領域に、電子キーの生成に使用される秘密キーｋを有する。この不揮発性メモリはさらに、電子キーのこの生成のためのこのプログラムを有する。このプログラムは公開キーF_Kの型の生成アルゴリズムを、秘密キーｋおよびそれに対応する公開キーＫを用いて実施する。　メモリ203はさらに、るカスタム化プログラムを含み、このプログラムは特定のデータ要素、すなわち、好ましい実施例ではカスタム化の日付D_pA（場合によっては時間も）の書込みで構成される。この情報は内部クロック204から得られる。　特定のデータ要素は新しいバージョンのキーごとにその値が増加する（増分は例えば１）カウンタ206によって得ることもできる。

これらのプログラムの実施はこの権限を与えられた人によるキーボード205によって開始される。　本発明の別の観点では、この揮発性メモリ203はこの公開キーＫＡと、権限の証明(certificate)ＣＥＲとを含むこともできる。　実際、生成器ＬＥに生成キーＣＬを生成する権限を与えなければならない。この権限の付与は、この機器には、認証機関ＡＴによって繰り返し行われる。実際には、認証機関はこの機器に公開キーＫを出力し、この公開キーＫはこのキーＣＬの計算においてこの機器によって使用される。しかし、このキーＫは、本明細書では保証ＣＥＲと称する署名によってこの機器に伝送される。　この保証ＣＥＲはしたがって、この許可された人の識別ＩＤ、彼の公開キーＫおよび有効性の時間ＶＡＬを含む一組のデータ要素のデジタル署名で、下記の如くである：　$CER=F_{KA}(ID, VAL, K)$　F_{KA}はこの公開キーアルゴリズムであり、ｋａはこの証明の計算用の秘密キーであり、ＫＡは対応する公開キーである。この計算は上記認証機関ＡＴによって行われる。この電子ロックＣＬはチップカード読取り機または上記の実施例のチップカード読取り機インターフェースを備えたマイクロコンピュータ型の機械によって生成される。　ロックＬは処理ユニット300と、電気的にプログラム可能な不揮発性メモリ301と、作業メモリ302とを有する。メモリ301は電子キーＣＬの検証する関数V_Kを実施するキーを検証するためのプログラムを有する。　このメモリ301はさらに、上記キーＣＬの生成に使用されている上記秘密キーｋに対応する上記公開キーＫを含む。　ロックＬは、本発明の第１の目的では、間違った電子キーの検証を可能にする。　このために、このロックは上記キーＣＬのカスタム化の日付D_pAと、同一のキャリヤ用に記憶されたカスタム化の日付とを比較する（ＩＤＡ識別）。　これらが一致する場合に、このロックはアクセスを許可する。日付D_pA＞上記ロックに存在するカスタム化の日付のときは、新しいバージョンのキーの場合である。このロックはそのキーのリストを更新する、すなわちカスタム化の新しい日付を古い日付の代わりに登録する。　上記日付D_pA＜上記ロックに存在する上記カスタム化の日付のときは、盗まれたあるいはなくしたと報告されたキーの再利用の場合である。アクセスは禁止される。キーの上記リストの更新はない。　権限ＨＡが割り当てられると、公開キーおよびキー生成器ＬＥの証明ＣＥＲの対と、キーＫＡはロック内の例えば作業メモリに記録され、このロックは権限の検証を行うことができる。　この検証は新しい権限ごとに行われる。このために、上記キーはさらに上記証明を検証するプログラムを含み、このプログラムは上記証明の検証関数V_{KA}を実施する。この検証の最後で、上記証明が上記公開キーＫに正しく対応している場合は、このキーはＥＥＰＲＯＭメモリに記録され、上記証明と上記キーＫＡは保存されない。　権限の変更が行われる場合、新しいキーＫ’用の証明ＣＥＲ’は上記認証機関ＡＴによって計算され、機器ＬＥにロードされる。その他の説明については、図２を参照することができる。　したがって、本発明の第２の目的では、権限のこのような変更は新しい公開キーＫ’の使用およびこの新しいキーＫ’の上記機器への割当てで構成される。　以前の公開キーＫを有していた上記機器によって計算された電子キーＣＬは、ロックがこの新しい権限を検証する限り、上記キーＫ’を有する機器によって生成された新しいキーと同様に常に有効である。　上記キーＫに割り当てられた有効期間は、有効性が終了する日が上記キーＫ’に割り当てられた有効期間の開始の日付またはこれより少し（例えば１ヶ月）後の日付になるように選択される。　生成器ＬＥが権限ＨＡ（ＩＤ，ＫＡ，ＣＥＲ，Ｋ）に関する

データ要素を有すし、それが最初の権限でもまたは新しい権限でも、生成されたキーＣＬ（Ｓ，D_pA，ＩＤＡ）が特定のデータ要素、例えば上記の生成されたキーが記録されるキャリヤのカスタム化の日付を有する場合には、上記ロックはこの説明の前の部分で述べたアクセス条件を検証し、さらに上記日付D_pAと上記機器の上記公開キーの有効性の時間とを比較することができる。この比較によって例えば、生成器ＬＥがもはや権限も持たないときに生成されたキーＣＬを検出することができる。　実際に、カスタム化の日付D_pAは上記キーＫまたはＫ’の有効期間ＶＡＬまたはＶＡＬ’のいずれかに強制的に帰する。　いずれの場合も、上記ロックは、上記のカスタム化の日付とそれに対応する公開キーのそれに対応する有効期間とを比較することができる。この検証の最後に、上記日付D_pAがそれに対応する公開キーの有効期間内にあることが認められる場合に、このロックはアクセスを許可する。　各公開キーＫまたはＫ’はこれに特有の有効期間を有するので、不正行為を検出するのが容易である。

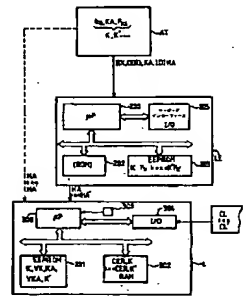
【図１】

FIG.1



【図２】

FIG.2



【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/FR 97/00676

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07C9/00 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07C G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 597 142 A (SCHLAGE LOCK COMPANY) 16 October 1987 see page 6, line 22 - page 11, line 11 see page 18, line 4 - page 19, line 18 see page 24, line 15 - page 26, line 32; figures 4,5,7-9	1-3,6,7
A	EP 0 605 996 A (FORD MOTOR COMPANY LIMITED) 13 July 1994 see column 3, line 7 - column 4, line 39; figure 1	1,5
A	EP 0 299 826 A (SCHLUMBERGER INDUSTRIES) 18 January 1989 see column 4, line 13 - column 8, line 8; figures 1,2	1-3

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 July 1997	22.07.97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Herbelet, J.C.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 97/00676

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 02899 A (GIRAULT,REITTER,REVILLET) 1 February 1996 cited in the application see page 6, line 12 - page 12, line 27; figures 1-3	1,2,6,7

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Ir tional Application No
PCT/FR 97/00676

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2597142 A	16-10-87	US 4837822 A	06-06-89
		AU 614715 B	12-09-91
		AU 7065287 A	15-10-87
		CA 1274608 A	25-09-90
		DE 3711746 A	15-10-87
		GB 2190523 A,B	18-11-87
		JP 7109144 B	22-11-95
		JP 62242079 A	22-10-87
		SE 8701411 A	09-10-87
EP 605996 A	13-07-94	JP 6245270 A	02-09-94
		US 5554977 A	10-09-96
EP 299826 A	18-01-89	FR 2618002 A	13-01-89
		JP 1093858 A	12-04-89
		US 4910774 A	20-03-90
WO 9602899 A	01-02-96	FR 2722596 A	19-01-96
		AU 2931795 A	16-02-96
		CA 2171626 A	01-02-96
		EP 0719438 A	03-07-96

フロントページの続き

(72)発明者　ジロー，マルク
フランス国　14000　カーン　リュ　ベル
ナールーヴァニエ　9
(72)発明者　レヴィエ，マリージョゼフ
フランス国　14790　ヴェルソン　リュ
ピショヴァン　11